Recent Developments Regarding U.S. and EU Regulation of Electronic Commerce

DAVID CHURCH, MIKE PULLEN, AND JANE K. WINN*

I. Introduction

The accelerating pace of business activity over global information networks such as the Internet raises many issues regarding the enforceability of contracts concluded over the networks, and the appropriate role of national governments in regulating that activity. While many enterprises are rolling out innovative business applications in the absence of clear guidance on applicable law, others are still waiting on the sidelines in the hope that the current turmoil surrounding developing business, technological, and legal models will subside. This article will summarize some major recent developments regarding the regulation of electronic commerce (EC) in the European Union, in the United States, and in selected multinational fora.

II. EC Directive

On November 18, 1998, the European Commission (Commission) proposed legislation in the form of a draft directive (Directive) designed to create a legal framework for electronic commerce (EC) within the European Union.[1] The aim of the legislation is to facilitate cross-border e-commerce transactions. The Directive incorporates the fundamental principles of the internal market, country of origin and mutual recognition. These principles have been reaffirmed

*David Church is the Managing Partner of Dibb Lupton Alsop Brussels office. He has been practicing in Brussels for over twelve years and has strong experience with EU and international legal issues. Mike Pullen is an Associate in the Dibb Lupton Alsop Brussels office. He specializes in EU internal market and competition law. He has particular expertise in e-commerce, data protection and media convergence issues under EU law. Jane K. Winn is an Associate Professor at Southern Methodist University School of Law, a member of the New York Bar and co-author of ELECTRONIC COMMERCE (3rd ed. 1998). She may be contacted at <http://www.smu.edu/~jwinn>; or <jwinn@mail.smu.edu>.

1. Proposal for a European Parliament and Council Directive on Certain Legal Aspects of Electronic Commerce in the Internal Markets, COM/98/0586 final (Nov. 18, 1998) *available in* LEXIS, Europe Library, Prep File.

by the European Court of Justice (ECJ) in a number of cases involving the free movement of goods and services beginning with the landmark *Cassis de Dijon* case.[2]

Before the EC Directive can have the force of law, it will have to be reviewed by the European Parliament, finalized by the Commission and promulgated by the European Council. Following enactment of the EC Directive by the European Union, the fifteen member states would be granted a period of time, normally two years, during which they would prepare and implement national legislation embodying the terms of the EC Directive. Thus, even if EU institutions handle the EC Directive expeditiously, it may be several years before harmonization of member state law in this area is achieved. If the Directive is adopted on the basis of the country or origin principle it will mean that businesses using e-commerce will only have to deal with one law, that of the country in which they are established, rather than up to fifteen different laws of the EU Member States. This is due to the fact that the concept of mutual recognition obliges EU Member States to accept that the laws of other member states provide a level of protection equal to their own law even if the laws of the other member states are different or less restrictive of certain activities.

A. Overview of the EC Directive

The Directive aims to address the current legal uncertainty surrounding the issue of establishment by providing a definition of the State of establishment in line with principles established by the EU Treaty and the case law of the ECJ. It also prohibits the use of prior licensing or special authorization schemes for e-commerce services and sets out certain information requirements that the service provider must give in order to ensure the transparency of its activities.

The Commission believes that commercial communications such as advertising, sponsorship, direct marketing, and promotion are a fundamental part of the majority of electronic commerce services. Therefore, the EC Directive defines what constitutes "commercial communication" and makes such communications subject to certain rules regarding transparency in order to ensure consumer confidence and fair trading. The Directive requires e-commerce businesses to ensure that commercial communications by e-mail are clearly identifiable in order to prevent harmful intrusion into consumer privacy.

The EC Directive also states that regulated professions (e.g., lawyers and accountants) should be permitted to use commercial communications providing they comply with the professional codes of conduct drawn up by national professional associations.

The Directive states that electronic commerce will not fully develop if the conclusion of on-line contracts is hampered by certain formal and other requirements (e.g., language requirements) that are not adapted to the needs of on-line business. The Directive proposes that member states should be obliged to adjust their national legislation to facilitate on-line contracts. In addition, the Directive clarifies the moment of the conclusion of a contract in certain cases.

The Commission recognizes the need to clearly identify the legal liability of on-line service providers for transmitting and storing third-party information. The EC Directive limits service provider liability by using the mechanism of a "mere conduit" for intermediary activities.

The Commission is seeking to ensure that existing EU and national legislation is effectively enforced. The EC Directive intends to do this by using the principle of mutual recognition and

2. Case 120/78, Rewe-Zentral AG contre Bundesmonopolverwaltung fur Brantwein, 1979 E.C.R. 649 (1979).

the development of codes of conduct at EU level. Furthermore, it aims to increase cross-border cooperation between national regulatory authorities in the member states and the setting up of an effective cross-border dispute resolution system.

B. Summary of Provisions of EC Directive

Article 1 of the EC Directive sets out its objectives and scope. It clarifies the primary objective which is to ensure that after the implementation of the Directive, e-commerce services will be able to fully benefit from the free movement of services between member states of the EU.

Article 2 gives definitions of what constitutes "information society services." This is in accordance with the definition laid down in articles 59 and 60 of the EU treaty. Information society services are defined as "any service that is normally provided for remuneration at a distance by electronic means and at the request of a recipient of services." The article also gives definitions of the terms "at a distance" by electronic means and "at the individual request of a recipient of services." The provision of Internet television broadcasting is expressly excluded from the definition as this is governed by article 1(a) of directive 89/552/EEC.

There is a certain amount of uninformed opinion surrounding the definition contained in article 2 which holds that services not provided for remuneration paid by the recipient fall outside the scope of the Directive. This is incorrect as the definition of services provided for remuneration is taken from articles 59 and 60 of the EU treaty and reaffirmed by the ECJ in *Bond van Adverteerders*,[3] where the ECJ stated that the term "provision of services for remuneration" covered services provided to recipients where remuneration was not given by the recipient but by a third party, e.g., an advertiser paying a TV broadcaster to transmit advertisements to the public is a service for remuneration despite the fact that the service is not paid for by the recipient. Article 2 also gives a definition of service providers which encompasses both natural and legal persons.

Paragraph (c) of article 2 defines the concept of "established service providers." This definition allows the Commission to determine the member state in whose jurisdiction the service provider is situated. It is based on article 52 of the EU treaty and the judgment of the ECJ in *Factortame*[4] where the ECJ stated that the concept of establishment within the meaning of article 52 of the treaty involves the actual pursuit of an economic activity through an establishment in a member state for an indefinite period. This definition is based on criteria regarding the nature and stability of the economic activity rather than formal legalistic criteria such as a letter box address or the establishment of a technical method of transmission.

It should also be noted that in certain circumstances the ECJ has held that a provider of services can be established in several member states. The ECJ has held that the member state in whose jurisdiction the service provider falls is the state where the service provider has its center of activities.[5] Article 2 also contains a definition of a recipient of services again based on articles 59 and 60 of the EU treaty.

The object of article 3 is the implementation of the freedom to provide services under article 59 of the EU treaty. This is based on determining the member state responsible for regulating the activities of e-commerce (the country of origin) and the prohibition on other member states restricting the freedom of e-commerce service providers to provide services (mutual recognition).

3. Case 352/85, Bond van Adverteerders v. Netherlands State, 1988 E.C.R. 2085 (1988).

4. Case 221/89, The Queen v. Secretary of State for Transport, *ex parte*, Factortame Ltd., 1991 E.C.R. I-3905 (1991).

5. *See* Case 56/96, VT4 Ltd. v. Vlaamse Gemeenschap, 1997 E.C.R. I-3143 (1997).

The member state in which the service provider is established pursuant to the definition in article 2 is required to ensure that the service provider's activities comply with the Directive as implemented into its national law.

This article does not override the 1980 Rome convention on applicable law for contractual obligations or the 1968 Brussels convention on jurisdiction and the enforcement of judgments.

The EC Directive includes provisions regarding the establishment and information requirements for electronic commerce activities. The purpose of article 4, governing the exclusion of prior authorization, is to reinforce the principle of freedom to provide services by facilitating access to the supply of services on the Internet. It constitutes a "right to a site" that can be exercised by any natural or legal person wishing to provide e-commerce services over the Internet. In short, this provision prevents member states from maintaining and introducing any legislation requiring prior authorization or licensing before internet sites can be set up for the provision of electronic commerce services. This article, however, does not override existing requirements for professional qualifications or authorizations by a professional body for the provision of services that are not exclusively aimed at e-commerce services.

Article 5, governing general information to be provided, sets out the minimum information (e.g., the name, place of establishment, e-mail address, and VAT registration) that the service provider must give to consumers. It supplements the information requirements that exist in directive 97/7/EC on the protection of consumers in relation to distance contracts. It also extends the provisions of the distance selling directive by placing the obligation on the service provider to provide the information even where no contract is to be formed. The information in question must be easily accessible from the service being provided (e.g., by clicking on an icon or a logo with hypertext link to the page containing the information that should be visible on all the pages of the website). Prices indicated in Euros will meet the price information requirement laid down in this article.

The EC Directive includes provisions governing commercial communications. Article 6 establishes the principle that commercial communications must be clearly identifiable as such by consumers. Commercial communications should not, for example, be hidden in the form of an advertorial. The person on whose behalf the commercial communication is carried out must also be clearly identified (e.g., the banner could carry the name of the company or an icon or logo with a hypertext link to the page containing this information that should be visible on all the pages of the site). Promotional offers must also be transparent and must give the consumer sufficient information so as not to leave any ambiguity as to their nature and the conditions of entry and participation.

The rules and conditions of entry to competitions and games must be clearly indicated to consumers by means of a logo or icon with a hypertext link to the relevant web page. It should be noted that the only competitions allowed under the Directive are those related to commercial communications. Article 22(1) expressly excludes gambling from the scope of the EC Directive.

The aim of article 7, which governs unsolicited commercial communications, is to ban spamming practices (i.e., the sending of unsolicited e-mail to consumers). This article obliges member states to enact legislation requiring unsolicited commercial communications to have a specific message on the envelope so that the recipient can immediately identify it as a commercial communication without having to open it.

Article 8, governing regulated professions, sets out the general principle that members of regulated professions are permitted to use commercial communication, to the extent necessary for these professions to be able to provide e-commerce services, provided that such communica-

tions meet the professional rules of conduct applicable to them. The Commission has also reserved the right to define what type of information is compatible with the professional rules of conduct in the committee set up under article 23.

The EC Directive includes provisions governing the treatment of electronic contracts. Article 9 requires member states to change their legislation in order to allow contracts to be concluded by electronic means. Member states will have to: (1) repeal provisions which expressly prohibit or restrict the use of electronic media for contracting; (2) refrain from preventing the use of certain electronic systems as intelligent electronic agents for making a contract; (3) refrain from creating a two-tier system that gives electronic contracts less legal effect than paper contracts; (4) repeal formal contractual requirements that cannot be met by electronic means or create ambiguities when applied to electronic contracts. (Note that this does not affect the requirement of a signature governed by the proposal for a directive on the common framework of electronic signatures.) Statements that the contract be "written" or that a document can be presented or that there is an original copy of the contract or that the contract must be "printed" or "published" will have to be amended as this will hinder electronic contracting.

Requirements that contracts be negotiated or concluded by natural persons or in the presence of both parties will also need to be changed to allow electronic contracting.

This article also contains a number of derogations from the general rules in respect to contracts requiring the involvement of a notary; contracts that must be registered with a public authority to be valid; contracts governed by family law; and contracts governed by the law of succession. The member states are required to submit complete lists of excluded contracts to the Commission.

In order to achieve a high standard of fair trading and consumer protection, article 10, governing information to be provided, sets out the different steps that are necessary to conclude an electronic contract. It requires member states to enact legislation for concluding an electronic contract using a mechanism to ensure that the parties can give full and valid consent.

The aim of article 11, governing the moment at which a contract is concluded, is to define with certainty when a contract is concluded. The contract is concluded when the recipient of the service has received from the service provider, electronically, an acknowledgment of receipt of the recipient's acceptance, and has confirmed receipt of the acknowledgement of receipt. Acknowledgment of receipt is deemed to be received and confirmation is deemed to have been given when the parties to whom they are addressed are able to access them. Acknowledgment of receipt by the service provider and confirmation of the service recipient shall be sent as quickly as possible.

The EC Directive also establishes limits on the liability of intermediaries. Article 12 creates an exemption from liability for service providers in situations where they act as a mere conduit for the transmission of information over a communications network. This exemption covers both cases in which a service provider would be directly liable and cases where the service provider would be considered secondly liable. This exemption from liability also includes criminal liability (e.g., a service provider would not be liable for the dissemination of pornographic material from a website connected to its system where it merely provided a conduit for the dissemination of the information over the Internet).

In order to qualify for the exemption, service providers must meet certain pre-conditions. The service provider must not initiate the transaction. This means that the transaction must not be under the control of the service provider. The service provider does not select the receivers of the transmission. The provider does not select nor modify the information contained in the transmission.

Article 13 governs temporary forms of storage which is referred to as "systems caching." This form of storage is used by service providers to enhance the performance of networks and does not constitute a separate use of information transmitted over the network; therefore copies of information made available on-line by third parties are temporarily kept in the operators system or network for the purpose of facilitating the access of subsequent users to the information. These copies are made by technical or automatic process and are intermediate between the network where the information was originally made available and the final user. In such cases the service provider shall not be liable providing that the following conditions are met: (a) the provider does not modify the information; (b) the provider complies with conditions on access to the information; (c) the provider complies with rules regarding the updating of the information, specified in a manner consistent with industrial standards; (d) the provider does not interfere with the technology, consistent with industrial standards, used to obtain data on the use of the information; and (e) the provider acts expeditiously to remove or to bar access to the information upon obtaining actual knowledge of one of the following.

Article 14 sets a limit on the liability of service providers as regards the activity for the storage of information provided by recipients of the service or at their request (e.g., the provision of server space for an individual website). The exemption from civil and criminal liability cannot be claimed if the service provider knows that the user of its service is undertaking illegal activity. The test is whether or not the service provider has actual knowledge of the illegal activity. The exemption from liability as regards complaints for civil damages will not be granted if the service provider is aware of the facts and circumstances from which the illegal activity is apparent. The test here is constructive knowledge. Service providers will not lose the exemption from liability if on obtaining actual or constructive knowledge of illegal activity they act expeditiously to remove or disable access to the information. The Commission also actively encourages industry self-regulatory mechanisms including the establishment of codes of conduct and hotline mechanisms to report illegal content.

Article 15 states that service providers are under no obligation to monitor third party content placed on their system. However this rule does not prevent a court or a law enforcement agency from requesting a service provider to monitor a site for a given period of time.

In article 16, the Commission is encouraging the creation of self-regulatory codes of conduct at EU level. In order to ensure that switch codes are consistent with EU law, interested parties are encouraged to inform the Commission of any draft codes. Voluntary agreements to which public authorities are party must be notified to the Commission in accordance with the terms of Directive 98/34/EC.

The EC Directive includes several provisions governing legal procedure and alternative dispute resolution processes. Article 17 seeks to establish a form of pan-European alternative dispute resolution for e-commerce transactions. The aim of article 18 is to ensure that member states take measures to ensure the availability of legal remedies in urgent cases (e.g., injunctions). The purpose of article 19 is to encourage cooperation between regulatory authorities in regulating the Internet. The aim of article 20 is to allow implementing measures to be adopted concerning the electronic means that might be considered appropriate for facilitating alternative dispute resolution and cooperation between the regulatory authorities and member states.

Article 21 includes a provision containing a standard EU requirement that member states put appropriate sanctions in place for violations of the EC Directive.

The EC Directive contains a number of derogations. Article 22 includes a general derogation that provides that the application of the Directive does not cover taxation and the free movement of personal data as guaranteed under directive 95/46/EC. Member states are also allowed to

derogate from the provisions of the Directive on the grounds of public policy, public security, public morality, and consumer protection. Derogations from article 3 are also allowed in respect to: (1) copyright, neighboring rights, rights referred to in Directive 87/64/EEC and Directive 96/9/EC as well as industrial property rights; (2) the emission of electronic money by institutions in respect of which member states have applied one of the derogations provided for in article 7(1) of Directive/EC; (3) article 44 paragraph 2 of Directive 85/611/EEC; (4) article 30 and Title IV of Directive 92/49/EEC, Title IV of Directive 92/96/EEC, articles 7 and 8 of Directive 88/357/EEC and article 4 of Directive 90/619/EEC; (5) contractual obligations concerning consumer contracts; and (6) unsolicited commercial communications by electronic mail, or by an equivalent individual communication. Before relying on such a derogation, however, a member state must inform the Commission.

Article 23 of the EC Directive sets up a consultative committee charged with assisting the Commission in implementing its power of enforcement.

C. Analysis of EC Directive

Perhaps the most contentious issues surrounding the adoption of the Directive are that it is based on the principles of mutual recognition and country of origin. Mutual recognition is an established and uncontroversial principle which is constantly applied in a multitude of sectors (e.g., the New Approach Directives on technical standards which apply to products including toy safety and low voltage). Despite this, consumer groups have attacked this aspect of the Directive. It seems surprising, if not perverse, that a concept that is uncontroversial when applied on a daily basis to product safety should become controversial when applied to the marketing of electronic services.

The Commission has chosen to use the principles of the country of origin and mutual recognition rather than full harmonization as the basis for the Directive because it recognizes member states of the EU operate a number of different sets of rules regarding marketing promotions and commercial communications which are impossible to harmonize without killing off the electronic commerce sector in its infancy. As a case in point, under the unfair competition laws of several member states (e.g., Germany) it is forbidden to offer three for the price of two discounts or loyalty bonuses. These types of restrictions are normally justified on the grounds of consumer protection. However, they are frequently characterized as restrictions on the freedom to trade which do nothing more than protect inefficient economic actors from fair competition. These laws have also been criticized as damaging to consumers interests as the restriction on the use of competitive tools such as promotions keeps prices at an artificially high level by discouraging new market entrants. This has been recognized by the Commission and it is taking a complaint against Germany for restricting the free movement of goods and services by imposing a ban on loyalty bonuses.

The decision to base the EC Directive on the principles of mutual recognition and country of origin will also help to overcome the setback suffered by the internal market when the ECJ delivered its ruling in the *Keck*[6] case, where it stated that restrictions on commercial communications which applied equally to both imported and domestic products and did not discriminate in law or in fact against traders fell outside the scope of article 30 of the treaty. This judgment has been used as a legal justification for the failure by the Commission

6. Joined Cases 267 & 268/91, Criminal Proceedings against Keck & Mithouard, 1993 E.C.R. I-6097 (1993).

to pursue infringement proceedings in respect of national laws that restrict the free movement of services. This is despite the fact that the ECJ has consistently refused to apply this principle to services under article 59. The ECJ's refusal to apply the *Keck* doctrine to the free movement of services is hardly surprising. The restrictions that the ECJ stated fall outside the scope of article 30 in the *Keck* judgment are secondary restrictions insofar as the free movement of goods is concerned, i.e., goods can still enter the market even though they cannot be marketed effectively. However, if this concept was to be applied to the free movement of services, it would constitute a primary barrier to free movement because services would not be allowed to cross borders. This would have the effect of fragmenting the internal market and distorting trade flows.

The EC Directive is a major step forward in increasing Europe's competitiveness in this rapidly developing area. It will allow a great deal of consumer choice, for example, a consumer in Member State A who is not able to take advantage of a three for the price of two offer through normal retailing channels in that state due to the existence of the unfair competition law may dial up a web site in Member State B and receive such an offer because the website established in Member State B will not be subject to the restrictions in Member State A.

Also, consumers will continue to enjoy a high level of protection as the EC Directive does not affect the provisions of other legislation such as the Distance Selling EC Directive, the Unfair Contract Terms Directive, and the Products Liability Directive, which impose an approximated set of rules for consumer protection across the EU. Consumers will also retain their right to sue suppliers in the consumers' country of domicile under the provisions of the Brussels Convention. Furthermore, contracts concluded between suppliers and consumers who are domiciled in different member states cannot be used to take away the rights protected under the terms of the Rome Convention which a consumer would enjoy in his country of domicile.

The EC Directive also allows member states to derogate from its provisions on a case-by-case basis to impose restrictions on information society services supplied from another member state if necessary to protect public interest on the grounds of protection of minors, fights against racial hatred, sexual racial discrimination, public health or security, and consumer protection. However, such restrictions must be proportionate to their stated objective. Moreover, it introduces the important caveat that the restrictions can only be imposed after (1) the member state where the service provider is established has been asked to take adequate measures and failed to do so, and (2) the intention to impose restrictions has been notified in advance to the Commission and to the member state where the service provider is established.

As stated above, the Directive has been strongly criticized by consumer groups. In the authors' view this criticism is based on a misunderstanding of the law. The consumer groups' view that the adoption of the EC Directive will have a negative effect on the present EU consumer protection legislation is mistaken. The fact of the matter is that the Directive actually strengthens EU consumer protection law by requiring, inter alia, transparency of commercial communications and increased cooperation between regulators. Therefore, the authors find it surprising that the consumer groups are taking such a negative view of a Directive that has many benefits for consumers while allowing the growth and expansion of businesses providing e-commerce services.

During the week ending on May 7, 1999, the EC Directive was given its first reading in the European Parliament. The Parliament supported the Commission's use of the principles of country of origin and mutual recognition as a basis for the Directive. However, the Parliament proposed a number of amendments to the Commission's text, the most controversial being the increase in the liability of Internet service providers for illegal content such as pornogrphy

or material breaching copyright. The original Commission proposal stated that Internet service providers would not be liable if they had no knowledge of the content stored on a website. However, the Parliament's proposed amendment states that providers will not be liable "if they do not know or are not in a position to know" that the activity carried out on a website is illegal. If the Parliament's amendment is accepted in its current form it will require the Internet service providers to monitor Internet traffic for illegal content. The service providers understandably have argued that monitoring would create problems, not least under the provisions of the Protection Directive and, assuming that monitoring of Internet traffic is technically feasible, the increased cost would be passed on to consumers, thus slowing down the development of e-commerce services within Europe. The Commission has stated that it will not accept this amendment and that it intends to back its original proposal.

III. E-Signature Directive

A. Overview and Summary of Provisions of the E-Signature Directive

In May 1998, the Commission put forward a proposal for a directive on electronic signature (E-Signature Directive).[7] The E-Signature Directive is designed to lay down minimum rules concerning security of electronic authentication technology and the liability of the parties using the technology in order to further develop the internal market through electronic commerce technologies. Various countries in Europe have already begun to enact laws prescribing diverging standards for electronic authentication technologies, so harmonization in this area is needed.[8] The Commission was instructed to draw up a directive governing digital signatures in particular, but instead issued a proposal based on the idea of an electronic signature in order to achieve a greater degree of neutrality among competing electronic authentication technologies.

The E-Signature Directive defines essential requirements for electronic signature certificates and certification services in order to ensure the interoperability of electronic commerce systems throughout the European Union.[9] The directive further provides that electronic signatures could not be discriminated against with regard to their legal effect solely because they are electronic.[10] Member states would not be permitted to require prior authorization before a certification service could be offered, although member states are free to set up voluntary accreditation schemes in order to standardize security levels offered to consumers of certification services.[11] Minimum liability rates would be established for providers of certifications services.[12] The E-Signature Directive does not address the requirements for authentication security within closed user groups, such as corporate intranets or banking systems, where the trust infrastructure is not so dependent on information technology and which may be subject to other regulations regarding on-line authentication.[13] The interoperability of EU certification systems with those

7. Proposal for a European Parliament and Council Directive on Common Framework for Electronic Signatures, COM/98/0297 final (May 13, 1998) *available in* LEXIS, Europe Library, Prep File [hereinafter Proposal on Electronic Signatures].

8. Germany, Italy, and France have enacted technology specific legislation that can be accessed from the Summary of Electronic Commerce and Digital Signature Legislation available at <http://www.mbc.com/ds_sum.html>.

9. Proposal on Electronic Signatures, *supra* note 7, arts. 2-4.

10. Proposal on Electronic Signatures, *supra* note 7, art. 5.

11. Proposal on Electronic Signatures, *supra* note 7, art. 3.

12. Proposal on Electronic Signatures, *supra* note 7, art. 3.

13. Proposal on Electronic Signatures, *supra* note 7, art. 6.

established in non-member states is to be promoted through a process for mutual recognition of certificates by bilateral or multilateral agreements.[14]

B. Analysis of E-Signature Directive

When the Council of Telecommunications Ministers met in November 1998, the E-Signature Directive failed to gain the support of all the member states.[15] Germany, Italy, France, and Portugal all supported a more technology specific approach, while the Commission and the remaining member states opposed such an approach. Until this conflict can be resolved, the directive is unlikely to be enacted in the near future. In addition, it is unclear that the E-Signature Directive can actually achieve its objective of neutrality among technologies. The E-Signature Directive can only achieve its stated objective of promoting the use of more reliable on-line authentication technologies if its provisions correspond with the actual commercial uses of this technology, which will not become apparent for some time.

IV. Update on Implementation of Data Protection Directive

A. Overview and Summary of Provisions of the Data Protection Directive

In 1995, the Council of Ministers and the Parliament of the European Union adopted a Data Protection Directive that provides individuals with powerful protections from nonconsensual uses of personal data.[16] The directive was designed to standardize the laws of the fifteen member states regarding the rights of individuals with regard to the privacy of personal information. The directive is based on the premise that privacy is a fundamental human right, and that the standardization of data protection laws in Europe must proceed on that basis. In addition to defining the content of that right within the European Union, the directive prohibits the transfer of personally identifiable data to non-EU countries that do not provide an adequate level of privacy protection. The approach to privacy rights taken in the directive is at odds with the prevailing approach in the United States, which is a piecemeal patchwork of different statutes, regulations, and caselaw that provides widely varying levels of protection to individuals depending on the context in which the personal information is collected or used.[17] As a result of these differences in basic philosophy and legal development, U.S. organizations collecting or using personal information about individuals in Europe have been very concerned about the impact of the adequacy standard as applied to types of data they receive from Europe. If such data is found not to be subject to an adequate level of protection once it has been transferred to the United States from Europe, the U.S. organizations face the prospect of interruptions in data flows or enforcement action taken by European data protection officials.

In order to be fully effective as law in the member states, each individual member nation must adopt legislation implementing the directive.[18] The directive was scheduled to become

14. *Electronic Commerce: Commission Proposes Electronic Signatures Directive*, RAPID, May 13, 1998 (Commission press release IP: 48/423) *available in* LEXIS News Library, Rapid File.

15. Proposal on Electronic Signatures, *supra*, note 7, art. 7.

16. Joe Kirwin, *EU Averts Clash With US; Fails to Agree to Legal Regime for Electronic Signatures*, BNA Electronic Com. & L. Rep., Dec. 9, 1998, at 1363.

17. Data Protection Directive, Council Directive 95/46/EC, 1995 O.J. (L 281) 31 [hereinafter DPD]. The text of the directive is available at <http://www.acs.ohio-state.edu/units/law/swire1/psecdir.htm.>.

18. For a summary of U.S. law, see Paul M. Schwartz & Joel R. Reidenberg, Data Privacy Law (1996). For an analysis of the DPD and how it is likely to be enforced, see Peter P. Swire & Robert E. Litan, None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive (1998).

effective on October 25, 1998; however, only four of the fifteen member states had passed the necessary legislation by that date. The slow pace of adoption of the directive within Europe notwithstanding, the lack of comprehensive privacy protection legislation in the United States has been a focal point for the attention of the European Commission in its preparations for the effective date of the directive.

The major provisions of the directive are aimed at guaranteeing that individuals remain in control of who collects and processes information and under what circumstances. The directive requires that personal data be collected only for specified, explicit, and legitimate purposes, that collections of data be maintained only to the degree that they are relevant to the purpose for which they were collected, and that data be maintained in an accurate and, where necessary, up-to-date form.[19] Subject to certain limited exceptions, the individual must provide unambiguous consent to the collection and use of personal information, unless an exception applies.[20] An exception to this requirement may apply if the data processing is necessary to accomplish some legitimate objective of the party in control of the data, in which case the individual is only entitled to be given notice and the opportunity to opt-out.[21] The individual must be able to determine who is in control of personal information relating to the individual, and the purposes for which the information will be used.[22] The individual is granted a right of access to personal information held by another party, and the individual must be able to exercise that right without excessive delay or expense.[23] The individual is also granted a right to correct inaccurate information, and a right of recourse in the event of unlawful collection or use of personal information.[24]

Having established a comprehensive system to protect the privacy rights of individuals in Europe, the directive goes on to restrict the circumstances under which personal information can be transferred out of Europe. Such transfers may take place only if the target country ensures an "adequate" level of protection.[25] The adequacy of the level of protection afforded by a third country depends on all the circumstances surrounding the transfer of personal information, and questions about the adequacy of levels of protection may be raised either by member states or the European Commission.[26] In the absence of an adequate level of protection, the transfer of data to a third country may nevertheless be permitted if the individual has unambiguously consented to the transfer, or the organization receiving the personal information has in place adequate safeguards based on contractual obligations.[27]

B. Analysis of Data Protection Directive

The Commission has indicated that current U.S. law protecting privacy rights does not provide an "adequate" level of protection for purposes of Article 25 of the directive. While representatives of the EU may believe that enactment of comprehensive privacy protection

19. For the sake of simplicity and clarity, this article will discuss the provisions of the DPD as though it was the applicable law, rather than discussing the provisions of specific national laws adopting the terms of the DPD, while recognizing the directive will not be fully effective until it is adopted by all members states.
20. DPD, *supra*, note 17, art. 6.
21. DPD, *supra*, note 17, art. 7.
22. DPD, *supra*, note 17, arts. 7, 14.
23. DPD, *supra*, note 17, art. 10.
24. DPD, *supra*, note 17, art. 12.
25. DPD, *supra*, note 17, arts. 12, 23.
26. DPD, *supra*, note 17, art. 25.
27. DPD, *supra*, note 17, art. 26.

laws in the United States is the most desirable solution to this problem, representatives of the United States believe that this is simply not a politically viable option. As a result, U.S. representatives have consistently advocated a solution to the problem of establishing that "adequate" levels of protection are available in the United States so that data flows will not be interrupted and U.S. organizations need not fear enforcement actions taken by members states based on self-regulation by U.S. organizations.

Representatives of the United States and European Union have been discussing for some time what the U.S. response to the directive will be, and the number and frequency of those discussions has accelerated as the effective date has come and gone without the differences between the U.S. and EU positions being resolved. The U.S. has consistently advocated self-regulation as an alternative to comprehensive national privacy legislation. The EU has indicated a willingness to consider such a strategy for resolving the differences between the two sides while at the same time expressed skepticism over the practical effectiveness of self-regulation in the United States in light of current practices. While the Department of Commerce has staunchly supported U.S. industry in advocating self-regulation as the solution to the conflict between U.S. and EU privacy law requirements, the U.S. Federal Trade Commission has also expressed skepticism over the practical effectiveness of self-regulation based on current U.S. privacy practices in the private sector. Representatives of the U.S. DOC and European Commission once hoped that their differences would be ironed out by the end of 1998, which coincidentally is the date given by FTC as the deadline for the private sector to demonstrate that self-regulation can be a viable alternative to federal legislation in this area.[28] Discussions between representatives of the Department of Commerce and the Commission have continued throughout the first half of 1999 and both sides expect to arrive at some resolution of the open issues by summer 1999.

V. Overview of Developments in U.S. EC Regulation

Among the first and most persistent commercial law issues raised by migrating business activity from paper-based administrative processes to electronic process have been the questions of what constitutes a writing or a signature. While these issues have been debated for more than a decade in the context of electronic data interchange (EDI) contracting, they have gained a new urgency in recent years with the commercial use of public key cryptography and digital signature technology. Signature and writing electronic commerce issues have already been addressed on an ad hoc basis in almost every state legislature. As a result, the National Conference of Commissioners on Uniform State Laws[29] (NCCUSL or the Uniform Law Commission) has taken steps to develop the Uniform Electronic Transactions Act (UETA) as a model state statute to build uniformity in this area, while at the same time, a frenzy of congressional lobbying for federal legislation in this area has erupted. Online contract formation issues are currently being addressed in the context of various uniform law drafting projects including the UETA, and revisions to UCC Article 2 on sale of goods. These issues are also addressed in the model law formerly known as UCC Article 2B, which, as of April 11, 1999, was removed from

28. Unless industry can demonstrate that it has developed and implemented broad-based and effective self-regulatory programs by the end of the year, additional governmental authority would be appropriate and necessary. *See* Testimony of Robert Pitofsky, Chairman of the Federal Trade Commission, before House Subcommittee on Telecommunications, Trade and Consumer Protection (July 20, 1998).

29. *See Uniform Law Commissioners* (visited Mar. 26, 1999) <http://www.nccusl.org>.

the UCC and renamed the Uniform Computer and Information Transactions Act (UCITA). Signature, writing and contract formation issues are also currently being debated in the European Union[30] and at the United Nations Commission on International Trade Law (UNCITRAL). In addition to these issues at the heart of contract law, novel legal issues are also being raised in other categories of commercial transactions such as secured transactions, payment systems, and transfers of documents of title.

A. Uniform Law Commission Projects

Since the widespread adoption of computer technology in business processes in the 1960s and 1970s, the Uniform Commercial Code (UCC) has undergone a series of revisions to try to adapt its provisions to maintain its relevance in light of case law developments and changing business practices. Revisions to the UCC are made under the joint sponsorship of the American Law Institute (ALI) and NCCUSL. Article 8 governing transfers in securities was first revised in 1977 to promote electronic clearing and settlement processes. Following the article 8 revision, attention was focused on article 3 governing negotiable instruments, article 4 governing check collection, and a new article 4A governing wholesale funds transfers, which were finalized in 1989. When the 1977 revisions to article 8 proved unworkable in practice, a new version of article 8 was prepared and finalized in 1994. Revisions to article 5 governing letters of credit were completed in 1994. In 1989, the process of revising UCC article 2 governing the sale of goods and article 9 governing secured transactions began.[31] In 1998, the revised version of article 9 was finalized. In 1994, the decision was made to bifurcate the article 2 revisions into work on article 2 governing the sale of goods, and work on a new article 2B governing software and information licensing, and it is expected that the revisions to article 2 will become final in 1999. The finalization of article 2B became problematic when serious concerns about its provisions were raised by the ALI. These concerns, however, lead to its reincarnation as UCITA, an independent model law that could be enacted by NCCUSL without the participation of the ALI.[32]

Signature and writing requirements have been among the many issues dealt with in most UCC revisions completed since 1990. Whenever a statute imposes a requirement of a signature by one of the parties or a written memorial of the transaction, parties will be reluctant to adopt electronic technology to substitute for paper-based processes. In the 1980s, parties wishing to sell goods subject to the UCC article 2 statute of frauds provisions[33] faced these problems with little or no hope of speedy legislative action to resolve them. A consensus emerged in favor of resolving these uncertainties through the use of a "trading partner agreement"—a traditional contract written on paper and manually signed by the parties proposing to use EDI for contracts between them.[34] The trading partner agreement specified the legal significance of subsequent electronic messages exchanged between the parties. This solution seems to have

30. *See* Sections I-III *supra*.

31. Drafts produced in the course of these and other current or very recent ULC projects are available at *The National Conference of Commissioners on Uniform State Laws* (visited Mar. 26, 1999) <http://www.law.upenn.edu/library/ulc/ulc.htm>.

32. Information about the provisions of proposed UCC Article 2B and the controversy surrounding them is available from *The 2B Guide* (visited Mar. 26, 1999) <http://www.2bguide.com>.

33. *See* UCC § 2-201 (1977).

34. One of the leading sources of information on electronic data interchange was published in *The Business Lawyer*. *See* Electronic Messaging Services Task Force, *The Commercial Use of Electronic Data Interchange: A Report and Model Trading Partner Agreement*, 45 Bus. Law. 1645 (1990).

worked well in managing the legal uncertainties surrounding EDI electronic commerce, since there are no reported cases involving EDI trading partner agreements.[35] In order to promote the harmonization of the commercial law governing EDI contracting for the benefit of parties participating in international transactions, in 1996, UNCITRAL promulgated a model law on electronic commerce.[36] The trading partner agreement solution is not suitable for environments in which it is not economical for transacting parties to execute a signed writing prior to the use of electronic contracting technologies.

In order to address those situations, the most recent revisions to the UCC have replaced references to writing with the word "record" and references to signature with the word "authentication." The definition of record is designed to be broad enough to include both electronic and paper documents without including highly transitory or intangible forms of communication, such as ephemeral sounds or smoke signals.[37] The definition of authentication is designed to be broad enough to include traditional manual signatures and electronic authentication systems without expanding the scope of the current definition of signature which requires some mark or symbol and an intent to be bound.[38] When these revisions become effective, many major obstacles to using electronic processes in business will have been removed. The problem is, however, that reforms to the UCC are proceeding slowly and do not have any legal effect until finally enacted by state legislatures. The degree of uniformity that will be achieved is also unclear, as it will not become clear for some time how widespread state support will be for the revisions to articles 2 and 9.

Given that not all commercial transactions are subject to the UCC, the Uniform Law Commission began a separate project outside the UCC to deal with other signature and writing requirements that currently exist under state law. Work began on the Uniform Electronic Transaction Act[39] in 1996, and is expected to be finalized in 1999. While the specific provisions of the statute will continue to change until it is finalized by NCCUSL, the main principles it adopts are now clear. This statute is designed to provide a transparent overlay of many existing state laws, and provides that transactions may not be denied legal effect just because they are executed in electronic form. The UETA does not require any person or organization to switch from

35. Explaining why the dog didn't bark is always a problematic venture, but it seems unlikely that reliance by the parties on trading partner agreements can be a complete explanation of why there is an absence of litigation in the EDI electronic contracting context. More important factors may be the increased accuracy and reliability of automated electronic contracting processes and the major investment most trading partners must make in making their information systems compatible before EDI messages can be exchanged at all gives trading partners an incentive to resolve disputes informally in order to preserve the value of that investment in interoperability.

36. *See Report of the United Nations Commission on International Trade Law on the Work of its Twenty-Ninth Session*, U.N. GAOR, 51st Sess., Supp. No. 17, Annex I at 70, U.N. Doc. A/51/17 (1996). The model law is available on the Internet at *UNCITRAL Model Law on Electronic Commerce* (visited Mar. 26, 1999) <http://www.un.or.at/uncitral/english/texts/electcom/ml-ec.htm>.

37. For example, the definition of record in 1998 Revised UCC § 9-102(69) provides: Except as used in "for record," "of record," "record or legal title," and "record owner," "record" means information that is inscribed on a tangible medium or which is stored in an electronic or other medium and is retrievable in perceivable form. *See* UCC § 9-102 (1998).

38. The current definition of signature in UCC § 1-201(39) provides "Signed" means any symbol executed or adopted by a party with present intention to authenticate a writing. *See* UCC § 1-201. As an example of the new definition of authenticate, 1998 Revised UCC § 9-102(7) provides: "Authenticate" means to: (A) sign; or (B) execute or adopt a symbol, or encrypt a record in whole or in part, with present intent to: (i) identify the authenticating party; and (ii) adopt, accept, or establish the authenticity of a record or term. *See* UCC § 9-102(7) (1998).

39. The most recent draft of the UETA is available at The National Conference of Commissioners on Uniform State Laws (visited Mar. 26, 1999) <http://www.law.upenn.edu/library/ulc/ulc.htm>.

paper to electronic media, and excludes from its scope certain categories of transactions that are not primarily commercial, such as wills. The UETA also provides that record keeping requirements currenting specify that records must be maintained in paper form may be met with electronic record storage technologies under appropriate circumstances. In keeping with the general approach taken in the UCC revisions, the UETA is designed to be media neutral and does not identify or favor any particular technology. Rather than promoting a particular form of electronic commerce, the UETA enables party choice and competitive markets to determine what technologies eventually become standards in electronic commerce.

This commitment to neutral enabling provisions in the UETA has led to a choice by its drafting committee to remain silent on questions of contract formation. In UCITA, by contrast, the decision has been made to provide more concrete guidance on issues such as contract formation to parties engaged in online commerce. Such provisions are felt to be appropriately within the scope of UCITA because online commerce is so important in the distribution of software and databases. These provisions also reflect a determination by the article 2B drafting committee that the uncertainty surrounding the legal effect of clicking on an "I agree" button on a computer screen was sufficient to warrant action to clarify the law in this area. The decision to make the enforceability of online contracts more certain, a move widely supported by the licensor groups such as the software industry, has raised a number of policy issues such as whether consumers and other licensees are adequately protected under the provisions of article 2B.

The UETA refrains not only from changing the substantive law of contract formation, it also refrains from assigning different legal significance to different electronic commerce technologies. This point is actually quite controversial since a great deal of lobbying and proselytizing in this area has been done by promoters of a specific technology, asymmetric (or public key) cryptography, and specific applications of that technology, digital signatures and public key infrastructures.[40] Promoters of this technology believe that it is without parallel as a solution to some of the problems encountered in trying to conduct business over the Internet or any other insecure public network.[41]

B. State Law

Since Utah passed the first state law recognizing the legal effect of digital signatures,[42] almost all fifty states have passed law of some description addressing signature and writing issues in electronic environments.[43] Many of these statutes have quite a limited scope, such as providing that a state government may accept documents in electronic form or digitally signed documents.[44] Some, following the Utah model, are highly regulatory in approach, providing for the legal consequences of using a specific technology in excruciating detail and including schemes to

40. For a general description of public key cryptography and digital signatures, *see, e.g.*, Benjamin Wright & Jane Winn, The Law of Electronic Commerce § 3.06 at [D] (3rd ed. 1998); Simson Garfinkel & Gene Spafford, Web Security and Commerce Ch. 10 (1998); Warwick Ford & Michael S. Baum, Secure Electronic Commerce (1997).

41. The ABA Science and Technology Committee's Digital Signature Guidelines (1996) is one of the leading examples of a work by supporters of public key cryptography, and is available at *ABA Section of Science & Technology Information Security Committee* (visited Mar. 26, 1999) <http://www.abanet.org/scitech/ec/isc/dsg.html>.

42. *See* Utah Digital Signature Act, Utah Code Ann. §§ 46-3-101–46-3-504 (1995).

43. A table of all state, federal, and foreign law dealing with digital signatures can be found at *MBC. Com* (visited Mar. 26, 1999) <http://www.mbc.com>.

44. *See, e.g.*, 1997 Texas House Bill 984, *codified at* Tex. Bus. & Com. Code Ann. § 2.108 (Vernon 1997).

license and audit providers of services integral to the use of the specified technology.[45] Other states have embraced the media neutral, enabling approach taken in the UETA,[46] while others have tried to combine a variety of approaches.[47] Although each state's action is designed to promote electronic commerce, those transactions may now take place anywhere within the entire U.S. market or within global markets, making cross-border harmonization of electronic commerce law highly desirable. While these statutes may be consistent on a number of issues and may flatly contradict on very few issues, the volume of legislation and the bewildering array of different approaches nevertheless makes it difficult for interested parties to determine their rights and obligations in this area. The Uniform Law Commission hopes that the UETA and the UCC revisions will help to remedy this situation, but even if those statutes are enacted by most or all states, it will be several years before the benefit of that greater uniformity reaches transacting parties. Due to concerns about the likelihood of relief at the state level, or the amount of time required to accomplish that, interested parties have begun lobbying Congress for federal legislation in this area.

C. U.S. Federal Law

In the 105th congressional session, many bills were introduced dealing with electronic commerce issues, but the only significant bill to become law was the Government Paperwork Elimination Act,[48] which permits the federal government to accept digital signatures. Among the bills that were not enacted were special interest legislation permitting regulated financial institutions to become major providers of online authentication services. This bill included provisions that would establish a self-regulatory organization to oversee providers of such services, similar to the role played by SROs such as the National Association of Securities Dealers in other financial services industries. While this bill was not enacted, it is clear that more legislation along the same lines will be introduced in the 106th Congress. The position of the Department of Commerce apparently is that with regard to the enforceability of contracts executed online, state laws such as the UETA are the most desirable alternative. With regard to establishing a more general regulatory framework to oversee the soundness of businesses providing the infrastructure of electronic commerce, there is not yet any consensus regarding its framework, let alone which institutions should provide it and how, if at all, their operations should be subject to government oversight.

Controls on the use of encryption technology is another area central to the regulation of electronic commerce in which many bills were introduced but no legislation enacted. Participants in the debate regarding government regulation of encryption technology were once limited to the military, law enforcement agencies, and civil libertarians.[49] In recent years, however, the adaptation of business computer systems to accommodate communications over open networks

45. *See* Utah Digital Signature Act, Utah Code Ann. §§ 46-3-201–46-3-204 (1995).

46. Legislation under consideration in Massachusetts takes this form. A draft of the proposed legislation is available at *Massachusetts Electronic Records & Signature Act* (visited Mar. 26, 1999) <http://www.state.ma.us/itd/legal/mersa.htm>.

47. Illinois Electronic Commerce Security Act, H.B. 3180, distinguishes between electronic signatures and records, and 'secure' electronic signatures and records, and assigns a different legal significance to each. It was enacted in 1998 and will become effective in 1999; the text of the law is available at *Illinois Electronic Commerce Legislation* (visited Mar. 26, 1999) <http://www.mbc.com/ceccmsg.html>.

48. It was enacted as part of Omnibus Appropriations Act, H.R. 4328, 105th Cong. (1998).

49. Stewart A. Baker & Paul R. Hurst, The Limits of Trust: Cryptography, Governments and Electronic Commerce 11 (1998).

such as the Internet has made the business use of sophisticated encryption technology routine. As a result, government efforts to require encryption technology vendors to build in backdoors to their security systems to permit possible government surveillance of users at some future date, or government restrictions on export of powerful encryption technology already in routine use within the United States, raise serious problems for information technology managers working to secure global enterprise communications networks. Business users of encryption technology have no choice but to try to navigate the hazardous terrain between the government's insistence that control of encryption technology is a matter of paramount concern to national security, and the insistence of civil liberties organizations that encryption technology is a constitutional right that must not be infringed in any way.[50]

Just as computer security was not an integral element of many routine business transactions before businesses began trying to execute those transactions online, concern for privacy rights was not an integral element of many routine business transactions. U.S. privacy law includes common law torts and many specific statutory provisions that apply to only limited categories of commercial activity, such as the Fair Credit Reporting Act, which governs the privacy rights of individuals with regard to their credit reports. As paper-based business processes are supplanted by electronic processes, and as more customers interact with businesses online, the volume of data that businesses can collect regarding their customers is expanding rapidly. Outside of industries such as health care or financial services, where the collection, analysis, and redistribution of personal data may be restricted by law, the collection of such data is not currently subject to regulation under U.S. law. Pressure to regulate the business use of personal data is growing in the United States in response to pressures from the European Union, concerned about cross-border flows of personal data about European citizens, from the Federal Trade Commission, exasperated with the failure of online merchants to adopt any meaningful form of self-regulation after having repeatedly undertaken to do so in order to avoid direct government regulation, and from U.S. consumers, concerned about the erosion of their privacy as businesses adopt more sophisticated technology. In 1998, legislation passed to stop unacceptable data collection practices among merchants operating Internet sites aimed at children, and it is likely that the FTC will introduce further legislation in this area in the 106th Congress.

V. International Developments Outside Europe

Electronic commerce conducted over the Internet has the potential to reach global markets for no greater cost in terms of investment in technology than that required to reach local communities. Unless progress is made in harmonizing the law that will apply to global Internet commerce, however, lack of certainty with regard to legal outcomes may be the one of greatest impediments to the development of that commerce. Recent efforts in the European Union to achieve harmonization in this area are covered in this symposium in a paper. In addition to a large number of initiatives taken by individual countries in this area,[51] UNCITRAL recently

50. For example, the Key Recovery Alliance is an association of business users of encryption technology seeking such a middle ground. Information about the Key Recovery Alliance is available at *Key Recovery Alliance* (visited Mar. 28, 1999) <http://www.kra.org>. Information about civil liberties groups who believe no government regulation of encryption technology is legitimate is available at the website of the Center for Democracy and Technology at *Center for Democracy & Technology* (visited Mar. 28, 1999) <http://www.cdt.org> and at Electronic Privacy Information Center website at *Epic.org* (visited Mar. 28, 1999) <http://www.epic.org>. The CDT and EPIC websites include information about current government policy initiatives in this area.

51. For a summary and overview of efforts by foreign countries, see *McBride, Baker & Coles* (visited Mar. 28, 1999) <http://www.mbc.com/ds_sum.html>.

completed a model law for electronic commerce, and is working on a model law for electronic signatures.[52]

The current efforts to produce a model law governing electronic signatures has proven controversial for the same reasons that consensus has been hard to achieve in this area among the different state governments in the United States. The United States and a limited number of other developed countries are advocating minimalist, technology neutral provisions, while a large number of other countries are pressing for a model law that assigns particular legal significance to digital signature technologies. While it is unclear how long it will take the Working Group on Electronic Commerce to produce a final product, in the interim, its deliberations are an interesting indicator of just how little consensus exists in this area at present.

On April 30, 1999, the World Intellectual Property Organization (WIPO) issued the WIPO Internet Domain Name Process final report dealing with some of the trademark law issues associated with Internet domain names.[53] This report includes recommendations designed to help protect the rights of trademark owners from abusive practices such as cybersquatting or domain name hijacking, in which an unrelated third party registers a domain name that suggests an existing trademark and then seeks compensation from the trademark holder in exchange for surrending the domain name. The proposals will be forwarded to the Internet Corporation for Assigned Names and Number (ICANN), the new private, not-for-profit organization established to take over the management of Internet domain names.[54] At this writing, the board of ICANN is scheduled to meet in May 1999, when it may adopt the proposals creating a new system for resolving trademark-related disputes regarding domain name registrations.

The main recommendations in the WIPO report include the establishment of a minimum "best practices" code for all generic top-level domain name registrars,[55] and the collection of contact information for domain name registration applicants so that intellectual property owners can contact them to enforce their rights; mandatory dispute settlement procedures to deal with cases of bad faith and abusive registration of domain names that violate trademark rights; and the creation of a system allowing owners of globally famous or well-known trademarks to obtain an exclusion prohibiting any person other than the trademark owner from registering domain names based on the mark.[56]

In October 1998, the Organization for Economic Cooperation and Development (OECD) held a ministerial conference in Ottawa, Canada to build a consensus among member countries on how to harness the enormous economic potential of electronic commerce and to ensure its continued growth in a socially responsible manner.[57] An agenda for establishing a global framework for electronic commerce was established, emphasizing freedom from taxation and reliance on market-based ordering rather than direct government regulation.

52. Information about UNCITRAL efforts is available at *Recent Documents of UNCITRAL and Its Working Groups* (visited Mar. 28, 1999) <http://www.un.or.at/uncitral/english/sessions/wg_ec/index.htm> and at *United Nations Commission on Int'l Trade Law* (visited Mar. 28, 1999) <http://www.mbc.com/legis/uncitral.html>.

53. WIPO Internet Domain Name Process Final Report (visited May 16, 1999) <http://wipo2.wipo.int/process/eng/processhome.html>.

54. For more information, see ICANN (visited May 16, 1999) <http://www.icann.org>.

55. Generic top-level domains include domain names ending in .com, .org, .net, .gov, or .edu.

56. Daniel Pruzin, *WIPO Issues Final Recommendation on Management of Internet Domain Names*, 4 BNA ELECTRONIC COM. & L. REP. 375 (1999).

57. Information on the OECD conference is available at <http://www.ottawaoecdconference.org> (visited May 16, 1999).

VI. American Bar Association Electronic Commerce Projects

At the time this was written, the ABA was engaged in a wide range of projects dealing with legal issues raised by electronic commerce conducted in global markets. The International Law Section is a co-sponsor of the ABA Jurisdiction in Cyberspace project. In 1999, the International Law and Practice Section established a special E-commerce Task Force that is drawing participants from all committees within the section. In addition, the Business Law Section Cyberspace Law Committee is addressing the problems of electronic commerce from many directions, as is the Science and Technology Section Electronic Commerce Committee.